IN THE CLAIMS:

Please cancel claims 1-39 and add new claims 40-65, as follows:

1.-39. (Canceled)

40. (New) A conditional access method wherein digitized multimedia data are transmitted in a continuous transport stream of successive data packets, comprising the steps of, at the generation side:

- selectively forming an encrypted transport stream from a base transport stream by detecting particular data packets within the base transport stream, removing and encrypting the particular data packets with an event encryption key, and

- inserting the encrypted data packets into the remaining base transport stream at insertion positions ahead in time with respect to the original positions of the particular data packets in the base transport system.

41. (New) The method of claim 40, comprising the step of buffering the non encrypted data packets while the particular data packets are encrypted.

42. (New) The method of claim 40, wherein the event decryption key is provided on a one-event smart card.

43. (New) The method of claim 40, wherein the event decryption key is provided on a one-limited-period smart card.

44. (New) The method of claim 40, comprising the step of transmitting the event decryption key in a Digital Video Broadcast DVB environment in specific Entitlement Management Messages EMMs protected by a user encryption key, the corresponding user decryption key being provided in the Control Access System CAS, on a user smart card or on a user Subscriber Identification Module SIM.

45. (New) The method of claim 40, wherein said encrypted data packets are inserted at positions a predetermined number of data packets ahead of respective original positions.

46. (New) The method of claim 40, wherein the decryption key is transmitted to a receiver with the selectively encrypted data stream.

47. (New) The method of claim 40, wherein the event decryption key is frequently changed.

48. (New) The system of claim 40, wherein the event decryption key is a fixed key distributed on a pay-per-event basis.

49. (New) The system of claim 40, comprising the step of transmitting the event decryption key via a mobile telecommunication network prior to broadcasting the multimedia data.

50. (New) The method of claim 40, comprising the step of providing the event decryption key encrypted by a user encryption key, and providing a corresponding user decryption key to an authorized user.

51. (New) The method of claim 40, wherein the encrypting step comprises the step of producing at a head-end encoder the selectively encrypted data stream, the head-end encoder including a Common Interface CI that in turn has a smart card SC interface for a smart card that has encryption circuitry thereon.

52. (New) The method of claim 40, wherein the encrypting step comprises the step of producing at a head-end encoder the selectively encrypted data stream, the head-end encoder including a Common Interface CI for a Personal Computer PC card module that has encryption circuitry thereon.

53. (New) The method of claim 40, wherein the encrypting step comprises the step of producing at a head-end encoder selectively encrypted data stream, the head-end encoder including a PC with an interface for a chip card containing an event encryption key or a user encryption key, the encryption being processed in the PC.

54. (New) The method of claim 40, wherein the encrypting step comprises the step of producing at a head-end encoder selectively encrypted data stream, the head-end encoder including an encoder CI module with a Common Interface and Transport Stream CI&TS interface to a professional Set-Top-Box STB.

55. (New) The method of claim 40, wherein the base data transport stream is a clear data

stream.

56. (New) The method of claim 40, wherein the base transport stream is a DVB-scrambled data stream.

57. (New) The method of claim 40, wherein all data packets other than the selectively encrypted data packets are DVB-scrambled.

58. (New) The method of claim 40, wherein every nth data packet of the transport stream is encrypted, n being a fixed number.

59. (New) The method of claim 40, wherein every nth data packet of the transport stream is encrypted, n being a variable number.

60. (New) The method of claim 59, wherein the variable number n is randomly variable.

61. (New) The method of claim 59, wherein the variable number n is variable as a function of data packet contents.

62. (New) The method of claim 40, further comprising the steps of, at the reception side :

- providing an event decryption key to an authorized receiver having a conditional access system,

- transmitting selectively the encrypted transport stream to the receiver,

- detecting the encrypted data packets by the conditional access system,

- removing the encrypted data packets from the received transport stream,

- decrypting the encrypted data packets with the event decryption key, and

- inserting the decrypted data packets into the remaining received transport stream at positions corresponding to the respective original positions of the particular data packets within the base transport stream.

63. (New) The method of claim 62, comprising the step of storing by the conditional access system into a buffer memory, clear data packets while decrypting an encrypted data packet.

64. (New) The method of claim 62, wherein said conditional access system includes a chip card with decryption circuitry thereon.

65. (New) The method of claim 64, wherein the chip card is a SIM card.